

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-141916

(43)Date of publication of application : 17.05.2002

(51)Int.Cl.

H04L 12/28

H04L 12/44

(21)Application number : 2000-337266

(71)Applicant : HITACHI CABLE LTD

(22)Date of filing : 31.10.2000

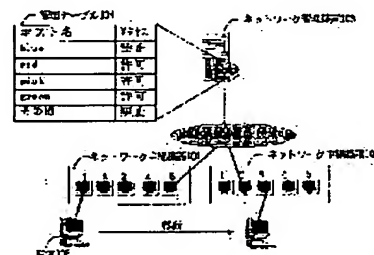
(72)Inventor : HIRAOKA DAIKI

(54) NETWORK MANAGEMENT SYSTEM, AND NETWORK REPEATER AND NETWORK MANAGEMENT DEVICE USED FOR THE SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a network management system ensuring the security, and a network repeater and a network management device used for the system.

SOLUTION: The network repeater 101 transmits information of a terminal 105 connected to the repeater 101 to the network management device 103, which returns information denoting an access permission/inhibition to the network repeater 101 depending on the terminal information, and the network repeater 101 sets use permission/use inhibit to a port to which the terminal 105 is connected based on the access permission/inhibition information. Since the permission/inhibition of the port to which the terminal 105 is connected is set depending on the terminal information managed by the network management device 103, the security is ensured without disturbing the use of a legal terminal.



## LEGAL STATUS

[Date of request for examination]

18.11.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-141916

(P 2 0 0 2 - 1 4 1 9 1 6 A)

(43) 公開日 平成14年5月17日(2002.5.17)

(51) Int. Cl. <sup>7</sup>

識別記号

F I

テ-マコード (参考)

H04L 12/28  
12/44

H04L 11/00

310

D 5K033

340

審査請求 未請求 請求項の数23 O L (全10頁)

(21) 出願番号 特願2000-337266(P 2000-337266)

(22) 出願日 平成12年10月31日(2000.10.31)

(71) 出願人 000005120

日立電線株式会社

東京都千代田区大手町一丁目6番1号

(72) 発明者 平岡 大樹

茨城県日立市砂沢町880番地 日立電線株式会社高砂工場内

(74) 代理人 100068021

弁理士 絹谷 信雄

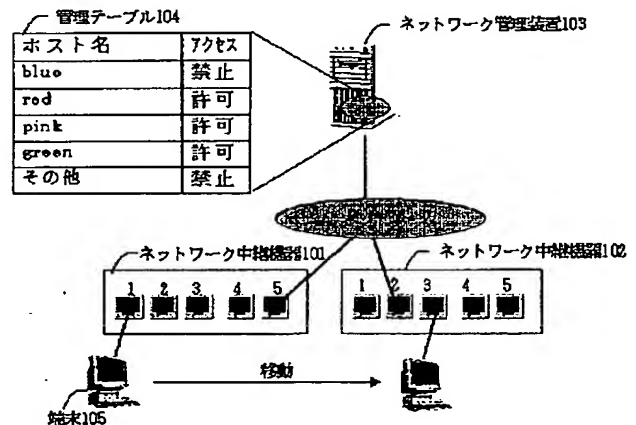
Fターム(参考) 5K033 BA04 BA08 DA05 DA15 DB12  
DB14 DB17 DB18 DB20 EA07  
EC01

(54) 【発明の名称】 ネットワーク管理システム並びにそれに用いるネットワーク中継機器及びネットワーク管理装置

(57) 【要約】

【課題】 セキュリティを確保できるネットワーク管理システム並びにそれに用いるネットワーク中継機器及びネットワーク管理装置を提供する。

【解決手段】 ネットワーク中継機器101より接続されている端末105の情報をネットワーク管理装置103に送信し、そのネットワーク管理装置103が前記端末情報に応じてアクセス許可/禁止を示す情報をネットワーク中継機器101に返信し、ネットワーク中継機器101が前記アクセス許可/禁止情報に基づいて端末105を接続しているポートを使用可能/使用不可に設定する。ネットワーク管理装置103が管理する端末情報に応じてネットワーク中継機器101のポートの使用可否が設定されるので、正当な端末の利用を妨げることなくセキュリティが確保される。



## 【特許請求の範囲】

【請求項 1】 ネットワーク中継機器より接続されている端末の情報をネットワーク管理装置に送信し、そのネットワーク管理装置が前記端末情報に応じてアクセス許可／禁止を示す情報を前記ネットワーク中継機器に返信し、前記ネットワーク中継機器が前記アクセス許可／禁止情報に基づいて端末を接続しているポートを使用可能／使用不可に設定することを特徴とするネットワーク管理システム。

【請求項 2】 前記端末情報は、当該端末を使用しているユーザの識別情報であることを特徴とする請求項 1 記載のネットワーク管理システム。

【請求項 3】 前記端末情報は、当該端末のホスト名であることを特徴とする請求項 1 記載のネットワーク管理システム。

【請求項 4】 前記端末情報は、当該端末の IP アドレスであることを特徴とする請求項 1 記載のネットワーク管理システム。

【請求項 5】 前記端末情報は、当該端末の MAC アドレスであることを特徴とする請求項 1 記載のネットワーク管理システム。

【請求項 6】 ネットワーク中継機器において、接続されている端末の情報をネットワーク管理装置に送信する機能を備えたことを特徴とするネットワーク中継機器。

【請求項 7】 前記端末情報の送信に対する返信として前記ネットワーク管理装置からアクセス許可／禁止を示す情報を受信した場合、このアクセス許可／禁止情報に基づいて端末を接続しているポートを使用可能／使用不可に設定する機能を備えたことを特徴とする請求項 6 記載のネットワーク中継機器。

【請求項 8】 前記端末情報をネットワーク管理装置に送信するポートと前記端末情報をネットワーク管理装置に送信しないポートとの設定がポート毎にできる機能を備えたことを特徴とする請求項 6 又は 7 記載のネットワーク中継機器。

【請求項 9】 前記端末情報をネットワーク管理装置に送信しないポートに対し任意にポートの使用可否が設定できる機能を備えたことを特徴とする請求項 8 記載のネットワーク中継機器。

【請求項 10】 前記端末情報をどのネットワーク管理装置に送信するかを指定しておくことができる機能を備えたことを特徴とする請求項 6 ～ 9 いずれか記載のネットワーク中継機器。

【請求項 11】 前記端末情報の送信に対する前記ネットワーク管理装置からの返信がなかった場合、端末が接続されているポートの使用可否が予め設定できる機能を備えたことを特徴とする請求項 6 ～ 10 いずれか記載のネットワーク中継機器。

【請求項 12】 前記端末情報は、当該端末が送信するデータの内容から取得した当該端末を使用しているユー

ザの識別情報であることを特徴とする請求項 6 ～ 11 いずれか記載のネットワーク中継機器。

【請求項 13】 前記端末情報は、当該端末が送信するデータの内容から取得した当該端末のホスト名であることを特徴とする請求項 6 ～ 11 のいずれか記載のネットワーク中継機器。

【請求項 14】 前記端末情報は、当該端末が送信するデータの内容から取得した当該端末の IP アドレスであることを特徴とする請求項 6 ～ 11 いずれか記載のネットワーク中継機器。

【請求項 15】 前記端末情報は、当該端末が送信するデータの内容から取得した当該端末の MAC アドレスであることを特徴とする請求項 6 ～ 11 いずれか記載のネットワーク中継機器。

【請求項 16】 ネットワーク管理装置において、ネットワーク中継機器から端末の情報を受信した場合、前記端末情報に応じてアクセス許可／禁止を示す情報を前記ネットワーク中継機器に返信する機能を備えたことを特徴とするネットワーク管理装置。

【請求項 17】 前記ネットワーク中継機器に返信するべきアクセス許可／禁止を示す情報と前記端末情報との対応を管理できる機能を備えたことを特徴とする請求項 16 記載のネットワーク管理装置。

【請求項 18】 前記端末情報は、当該端末を使用しているユーザの識別情報であることを特徴とする請求項 16 又は 17 記載のネットワーク管理装置。

【請求項 19】 前記端末情報は、当該端末のホスト名であることを特徴とする請求項 16 又は 17 記載のネットワーク管理装置。

【請求項 20】 前記端末情報は、当該端末の IP アドレスであることを特徴とする請求項 16 又は 17 記載のネットワーク管理装置。

【請求項 21】 前記端末情報は、当該端末の MAC アドレスであることを特徴とする請求項 16 又は 17 記載のネットワーク管理装置。

【請求項 22】 IP アドレスと有効ビットマスク値とを組として複数の IP アドレスを指定する IP サブネットを用い、この IP サブネットとアクセス許可／禁止情報との対応を定義しておき、この定義に照らして前記アクセス許可／禁止情報と前記端末の IP アドレスとの対応を管理する機能を備えたことを特徴とする請求項 20 記載のネットワーク管理装置。

【請求項 23】 前記ネットワーク中継機器からの送信及びその送信に対する返信の内容をログとして記録し、このログを管理画面から参照できる機能を備えたことを特徴とする請求項 16 ～ 22 いずれか記載のネットワーク管理装置。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】 本発明は、ネットワーク中継

機器を用いたネットワーク管理システムに係り、特に、セキュリティを確保できるネットワーク管理システム並びにそれに用いるネットワーク中継機器及びネットワーク管理装置に関するものである。

【 0 0 0 2 】

【従来の技術】多くのネットワーク中継機器は、ポートの使用可否の設定機能を備えている。ポートを使用不可に設定すると、そのポートに接続されたネットワーク機器は前記ネットワーク中継機器を介して通信を行うことができない。

【 0 0 0 3 】

【発明が解決しようとする課題】ネットワーク上に設置されているネットワーク中継機器に、どの端末を接続しても、ポートが使用可能に設定されていれば、その端末は前記ネットワーク中継機器を介して通信を行うことができる。仮に、悪意を持った外部からの侵入者の端末でも同様に通信を行うことができる。侵入者の端末がネットワークにアクセスできないようポートを使用不可に設定すると、本来、ネットワークにアクセスが許されるべき端末をもネットワークにアクセスさせないことになってしまう。このように、従来のネットワーク中継機器を用いたネットワーク管理システムではセキュリティの確保が難しい。

【 0 0 0 4 】そこで、本発明の目的は、上記課題を解決し、セキュリティを確保できるネットワーク管理システム並びにそれに用いるネットワーク中継機器及びネットワーク管理装置を提供することにある。

【 0 0 0 5 】

【課題を解決するための手段】上記目的を達成するために本発明のネットワーク管理装置は、ネットワーク中継機器より接続されている端末の情報をネットワーク管理装置に送信し、そのネットワーク管理装置が前記端末情報に応じてアクセス許可／禁止を示す情報を前記ネットワーク中継機器に返信し、前記ネットワーク中継機器が前記アクセス許可／禁止情報に基づいて端末を接続しているポートを使用可能／使用不可に設定するものである。

【 0 0 0 6 】前記端末情報は、当該端末を使用しているユーザの識別情報であってもよい。

【 0 0 0 7 】前記端末情報は、当該端末のホスト名であってもよい。

【 0 0 0 8 】前記端末情報は、当該端末の I P アドレスであってもよい。

【 0 0 0 9 】前記端末情報は、当該端末の M A C アドレスであってもよい。

【 0 0 1 0 】また、本発明のネットワーク中継機器は、接続されている端末の情報をネットワーク管理装置に送信する機能を備えたものである。

【 0 0 1 1 】前記端末情報の送信に対する返信として前記ネットワーク管理装置からアクセス許可／禁止を示す

情報を受信した場合、このアクセス許可／禁止情報に基づいて端末を接続しているポートを使用可能／使用不可に設定する機能を備えてもよい。

【 0 0 1 2 】前記端末情報をネットワーク管理装置に送信するポートと前記端末情報をネットワーク管理装置に送信しないポートとの設定がポート毎にできる機能を備えてもよい。

【 0 0 1 3 】前記端末情報をネットワーク管理装置に送信しないポートに対し任意にポートの使用可否が設定できる機能を備えてもよい。

【 0 0 1 4 】前記端末情報をどのネットワーク管理装置に送信するかを指定しておくことができる機能を備えてもよい。

【 0 0 1 5 】前記端末情報の送信に対する前記ネットワーク管理装置からの返信がなかった場合、端末が接続されているポートの使用可否が予め設定できる機能を備えてもよい。

【 0 0 1 6 】前記端末情報は、当該端末が送信するデータの内容から取得した当該端末を使用しているユーザの識別情報であってもよい。

【 0 0 1 7 】前記端末情報は、当該端末が送信するデータの内容から取得した当該端末のホスト名であってもよい。

【 0 0 1 8 】前記端末情報は、当該端末が送信するデータの内容から取得した当該端末の I P アドレスであってもよい。

【 0 0 1 9 】前記端末情報は、当該端末が送信するデータの内容から取得した当該端末の M A C アドレスであってもよい。

【 0 0 2 0 】また、本発明のネットワーク管理装置は、ネットワーク中継機器から端末の情報を受信した場合、前記端末情報に応じてアクセス許可／禁止を示す情報を前記ネットワーク中継機器に返信する機能を備えたものである。

【 0 0 2 1 】前記ネットワーク中継機器に返信するべきアクセス許可／禁止を示す情報と前記端末情報との対応を管理できる機能を備えてもよい。

【 0 0 2 2 】前記端末情報は、当該端末を使用しているユーザの識別情報であってもよい。

【 0 0 2 3 】前記端末情報は、当該端末のホスト名であってもよい。

【 0 0 2 4 】前記端末情報は、当該端末の I P アドレスであってもよい。

【 0 0 2 5 】前記端末情報は、当該端末の M A C アドレスであってもよい。

【 0 0 2 6 】 I P アドレスと有効ビットマスク値とを組として複数の I P アドレスを指定する I P サブネットを用い、この I P サブネットとアクセス許可／禁止情報との対応を定義しておき、この定義に照らして前記アクセス許可／禁止情報と前記端末の I P アドレスとの対応を

管理する機能を備えてもよい。

【0027】前記ネットワーク中継機器からの送信及びその送信に対する返信の内容をログとして記録し、このログを管理画面から参照できる機能を備えてもよい。

【0028】

【発明の実施の形態】以下、本発明の実施形態を添付図面に基いて詳述する。

【0029】1) 第一の実施形態

図1に示されるように、本発明に係るネットワーク管理システムは、本発明に係る2台のネットワーク中継機器101、102と、本発明に係るネットワーク管理装置103とを有する。ネットワーク中継機器は、例えば、スイッチングハブである。

【0030】図2に示されるように、スイッチングハブ201は、1番～5番ポート202～206、中継回路207、プロセッサ208、メモリ209等から構成されている。

【0031】以下に、スイッチングハブ201等のネットワーク中継機器が行う処理及びネットワーク中継機器に対して管理者が行う処理を示す。

【0032】(1) 管理者は、予めポート毎に、端末が接続された場合に、その端末の情報をネットワーク管理装置に送信するかどうかを設定しておく。端末情報を送信するポートを以下、自動使用可否設定ポートと呼ぶ。

【0033】(2) 管理者は、自動使用可否設定ポートでないポートについて、その使用可否を予め設定しておく。

【0034】(3) 管理者は、端末情報の送信先となるネットワーク管理装置のアドレスを予め設定しておく。

【0035】(4) ネットワーク中継機器は、自動使用可否設定ポートに新たに端末が接続された場合など、端末情報を送信するべき際、自動使用可否設定ポートが受信したフレームからホスト名等の端末を識別するための識別キーを検出し、その識別キーを端末情報としてネットワーク管理装置に送信する。

【0036】(5) ネットワーク中継機器は、端末情報の送信に対する返信としてネットワーク管理装置からアクセス許可を示す情報を受信した場合、端末が接続されているポートを使用可能に設定する。

【0037】(6) ネットワーク中継機器は、端末情報の送信に対する返信としてネットワーク管理装置からアクセス禁止を示す情報を受信した場合、端末が接続されているポートを使用不可に設定する。

【0038】(7) ネットワーク中継機器は、ネットワーク管理装置に端末情報を送信した後、ネットワーク管理装置から返信がなかった場合、この場合のために予め指定してあったとおりに使用可否の設定を行う。

【0039】(8) 以上によって設定された各設定内容(ネットワーク中継機器の構成情報と呼ぶ)はメモリ209に格納される。爾後、中継回路207は、ネットワ

ーク中継機器201の構成情報を通信処理に使用する。

【0040】以下に、ネットワーク管理装置103が行う処理を示す。

【0041】(1) 各端末とポートの使用可否との管理テーブル(ホスト名とアクセス許可/禁止情報とを対応させて登録したもの)104を内部に持っており、管理画面上からこの管理テーブルの設定ができる。

【0042】(2) ネットワーク中継機器から端末情報である識別キー(ホスト名)が送信された場合、管理テーブル104から端末を検索し、アクセス許可またはアクセス禁止を示す情報を前記ネットワーク中継機器に返信する。

【0043】(3) ネットワーク中継機器からの問い合わせ(端末情報を送信すること)及びその問い合わせに対する返信の内容をログとして記録する。このログは、管理画面から参照できる。

【0044】図1を用いて、より具体的な流れを説明する。ここでは、端末情報は端末のホスト名である。

【0045】ネットワーク中継機器101の1番ポート～4番ポート及びネットワーク中継機器102の1番ポート、3番ポート～5番ポートは、自動使用可否設定ポートに設定されているものとする。ネットワーク中継機器101の5番ポート及びネットワーク中継機器102の2番ポートは、自機及び接続される端末が上位ネットワークと通信できるように使用可能に設定されているものとする。

【0046】また、ネットワーク中継機器101、102には、端末情報の送信先となるネットワーク管理装置のアドレスとしてネットワーク管理装置103のアドレスが設定されているものとする。

【0047】ネットワーク管理装置103には、図示のように、予め内部の管理テーブル104に設定がなされているものとする。

【0048】いま、ホスト名がredの端末105がネットワーク中継機器101の1番ポートに接続されたとする。端末105からフレームが送信されると、ネットワーク中継機器101のフィルタリングテーブル(図示せず)にフレームから抽出した端末105のMACアドレスが登録される。そのタイミングでネットワーク中継機器101は、端末105のIPアドレスを検出し、DNSによりホスト名を検索し、そのホスト名をネットワーク管理装置103に送信する。

【0049】ネットワーク管理装置103は、受信したホスト名に対応したデータを管理テーブル104から検索する。ホスト名redは、アクセスが許可と設定されているので、ネットワーク管理装置103は、アクセス許可を示す情報をネットワーク中継機器101に返信する。

【0050】アクセス許可を示す情報を受信したネットワーク中継機器101は、端末105が接続されている

1番ポートを使用可能にする。これにより、端末105は、ネットワーク中継機器101を介してネットワークにアクセスすることができるようになる。

【0051】同様に、ホスト名がredの端末105がネットワーク中継機器102の3番ポートに接続された場合も、ネットワーク中継機器102の3番ポートは利用可能に設定される。つまり、この端末105は、どのネットワーク中継機器のどのポートに接続しても、ネットワークにアクセスすることができることになる。

【0052】端末105のホスト名がblueの場合、管理テーブル104にアクセスが禁止と設定されているので、ネットワーク中継機器101、102からの問い合わせに対してネットワーク管理装置103からアクセス禁止を示す情報が返信される。アクセス禁止を示す情報を受信したネットワーク中継機器101、102は、端末105が接続されているポートを使用不可にする。これにより、端末105は、ネットワーク中継機器101、102を介してネットワークにアクセスすることができない。

【0053】端末105のホスト名がgrayの場合、管理テーブル104に該当するホスト名が登録されていないため、管理テーブル104の“その他”のデータが参照され、そのデータにはアクセスが禁止と設定されているので、ネットワーク中継機器101、102からの問い合わせに対してネットワーク管理装置103からアクセス禁止を示す情報が返信される。ネットワーク中継機器101、102は、端末105が接続されているポートを使用不可にするので、端末105は、ネットワーク中継機器101、102を介してネットワークにアクセスすることができない。これにより、不明なホスト名が設定されている端末をネットワークにアクセスさせることを防ぐことができる。

【0054】以上のネットワーク中継機器からの問い合わせ及び返信の内容はネットワーク管理装置103に記録され、後に管理者がそのログを管理画面から参照することができる。

【0055】ネットワーク中継機器101、102とネットワーク管理装置103との通信ができなかった場合など、端末情報の送信に対する返信がなかった場合、ネットワーク中継機器101、102は、このような場合のために予め指定してあった通りにポートの使用可否を設定する。

【0056】このようにして設定されたネットワーク中継機器の構成情報は、メモリ209に格納され、中継回路207によって通信処理に使用される。

#### 【0057】2) 第二の実施形態

図3に示されるように、本発明に係るネットワーク管理システムは、本発明に係る2台のネットワーク中継機器101、102と、本発明に係るネットワーク管理装置103とを有する。ネットワーク中継機器は、例えば、

スイッチングハブであり、図2に示した内部構成を有する。

【0058】以下に、スイッチングハブ201等のネットワーク中継機器が行う処理及びネットワーク中継機器に対して管理者が行う処理を示す。

【0059】(1) 管理者は、予めポート毎に、そのポートで受信したデータの内容から端末使用者のユーザID(識別情報)を検知した場合にそのユーザIDを端末情報としてネットワーク管理装置に送信するかどうかを設定しておく。検知したユーザIDを送信するポートを以下、自動使用可否設定ポートと呼ぶ。

【0060】(2) 管理者は、自動使用可否設定ポートでないポートについて、その使用可否を予め設定しておく。

【0061】(3) 管理者は、ユーザIDの送信先となるネットワーク管理装置のアドレスを予め設定しておく。

【0062】(4) ネットワーク中継機器は、あるポートで受信したデータの内容から端末使用者のユーザIDを検知した場合、そのユーザIDを端末情報としてネットワーク管理装置に送信する。

【0063】(5) ネットワーク中継機器は、ユーザIDの送信に対する返信としてネットワーク管理装置からアクセス許可を示す情報を受信した場合、端末が接続されているポートを使用可能に設定する。

【0064】(6) ネットワーク中継機器は、ユーザIDの送信に対する返信としてネットワーク管理装置からアクセス禁止を示す情報を受信した場合、端末が接続されているポートを使用不可に設定する。

【0065】(7) ネットワーク中継機器は、ネットワーク管理装置にユーザIDを送信した後、ネットワーク管理装置から返信がなかった場合、この場合のために予め指定してあった通りに使用可否の設定を行う。

【0066】(8) 以上によって設定されたネットワーク中継機器の構成情報はメモリ209に格納される。爾後、中継回路207は、ネットワーク中継機器の構成情報を通信処理に使用する。

【0067】以下に、ネットワーク管理装置103が行う処理を示す。

【0068】(1) 各ユーザIDとポートの使用可否との管理テーブル(ユーザIDとアクセス許可/禁止情報とを対応させて登録したもの)104を内部に持っており、管理画面上からこの管理テーブル104の設定ができる。

【0069】(2) ネットワーク中継機器から端末情報であるユーザIDが送信された場合、管理テーブル104から端末を検索し、アクセス許可またはアクセス禁止を示す情報を前記ネットワーク中継機器に返信する。

【0070】(3) ネットワーク中継機器からの問い合わせ及びその問い合わせに対する返信の内容をログとし

て記録する。このログは、管理画面から参照できる。

【0071】図3を用いて、より具体的な流れを説明する。

【0072】ネットワーク中継機器101の1番ポート～4番ポート及びネットワーク中継機器102の1番ポート、3番ポート～5番ポートは、自動使用可否設定ポートに設定されているものとする。ネットワーク中継機器101の5番ポート及びネットワーク中継機器102の2番ポートは、自機及び接続される端末が上位ネットワークと通信できるように使用可能に設定されているものとする。

【0073】また、ネットワーク中継機器101、102には、ユーザIDの送信先となるネットワーク管理装置のアドレスとしてネットワーク管理装置103のアドレスが設定されているものとする。

【0074】ネットワーク管理装置103には、図示のように、予め内部の管理テーブル104に設定がなされているものとする。

【0075】いま、端末105がネットワーク中継機器101の1番ポートに接続されていたとする。ログイン名“Yamamoto”のユーザIDを持つユーザが端末105にログインすると、端末105からログイン情報を持つフレームが送信されるので、ネットワーク中継機器101は、そのフレームからユーザID“Yamamoto”を検出し、このユーザIDをネットワーク管理装置103に送信する。

【0076】ネットワーク管理装置103は、受信したユーザIDに対応したデータを管理テーブル104から検索する。この例では、ユーザID“Yamamoto”に対しアクセスが許可と設定されているので、ネットワーク管理装置103は、アクセス許可を示す情報をネットワーク中継機器101に返信する。

【0077】アクセス許可を示す情報を受信したネットワーク中継機器101は、端末105が接続されている1番ポートを使用可能にする。これにより、端末105は、ネットワーク中継機器101を介してネットワークにアクセスすることができるようになる。

【0078】同様に、端末105がネットワーク中継機器102の3番ポートに接続された場合も、“Yamamoto”のユーザIDを持つユーザがログインすれば、ネットワーク中継機器102の3番ポートは利用可能に設定される。

【0079】また、ネットワーク中継機器102の5番ポートに接続された別の端末106に“Yamamoto”のユーザIDを持つユーザがログインした場合も、ネットワーク中継機器102の5番ポートは利用可能に設定される。つまり、ユーザID“Yamamoto”を使用するユーザは、どの端末を使用しても、また端末をどのネットワーク中継機器のどのポートに接続しても、ネットワークにアクセスすることができることにな

る。

【0080】端末105のユーザIDが“Kawaguti”の場合、管理テーブル104にアクセスが禁止と設定されているので、ネットワーク中継機器101、102からの問い合わせに対してネットワーク管理装置103からアクセス禁止を示す情報が返信される。アクセス禁止を示す情報を受信したネットワーク中継機器101、102は、端末105が接続されているポートを使用不可にする。これにより、端末105は、ネットワーク中継機器101、102を介してネットワークにアクセスすることができない。

【0081】端末105のユーザIDが“Yamada”の場合、管理テーブル104に該当するユーザIDが登録されていないため、管理テーブル104の“その他”のデータが参照され、そのデータにはアクセスが禁止と設定されているので、ネットワーク中継機器101、102からの問い合わせに対してネットワーク管理装置103からアクセス禁止を示す情報が返信される。ネットワーク中継機器101、102は、端末105が接続されているポートを使用不可にするので、端末105は、ネットワーク中継機器101、102を介してネットワークにアクセスすることができない。これにより、不明なユーザIDを使用してログインされる端末をネットワークにアクセスさせることを防ぐことができる。

【0082】以上のネットワーク中継機器からの問い合わせ及び返信の内容はネットワーク管理装置103に記録され、後に管理者がそのログを管理画面から参照することができる。

【0083】ネットワーク中継機器101、102とネットワーク管理装置103との通信ができなかった場合など、端末情報の送信に対する返信がなかった場合、ネットワーク中継機器101、102は、このような場合のために予め指定してあった通りにポートの使用可否を設定する。

【0084】このようにして設定されたネットワーク中継機器の構成情報は、メモリ209に格納され、中継回路207によって通信処理に使用される。

【0085】3) 第三の実施形態

図4に示されるように、本発明に係るネットワーク管理システムは、本発明に係る2台のネットワーク中継機器101、102と、本発明に係るネットワーク管理装置103とを有する。ネットワーク中継機器は、例えば、スイッチングハブであり、図2に示した内部構成を有する。

【0086】以下に、スイッチングハブ201等のネットワーク中継機器が行う処理及びネットワーク中継機器に対して管理者が行う処理を示す。

【0087】(1) 管理者は、予めポート毎に、端末が接続された場合に、その端末のIPアドレスを端末情報



としてネットワーク管理装置に送信するかどうかを設定しておく。端末情報を送信するポートを以下、自動使用可否設定ポートと呼ぶ。

【0088】(2) 管理者は、自動使用可否設定ポートでないポートについて、その使用可否を予め設定しておく。

【0089】(3) 管理者は、IPアドレスの送信先となるネットワーク管理装置のアドレスを予め設定しておく。

【0090】(4) ネットワーク中継機器は、フィルタリングテーブル(図示せず)に新たにMACアドレスが登録される場合など、端末のIPアドレスを送信するべき際、自動使用可否設定ポートが受信したフレームから端末のIPアドレスを検出し、そのIPアドレスをネットワーク管理装置に送信する。

【0091】(5) ネットワーク中継機器は、IPアドレスの送信に対する返信としてネットワーク管理装置からアクセス許可を示す情報を受信した場合、端末が接続されているポートを使用可能に設定する。

【0092】(6) ネットワーク中継機器は、IPアドレスの送信に対する返信としてネットワーク管理装置からアクセス禁止を示す情報を受信した場合、端末が接続されているポートを使用不可に設定する。

【0093】(7) ネットワーク中継機器は、ネットワーク管理装置にIPアドレスを送信した後、ネットワーク管理装置から返信がなかった場合、この場合のために予め指定してあったとおりに使用可否の設定を行う。

【0094】(8) 以上によって設定されたネットワーク中継機器の構成情報はメモリ209に格納される。爾後、中継回路207は、ネットワーク中継機器201の構成情報を通信処理に使用する。

【0095】以下に、ネットワーク管理装置103が行う処理を示す。

【0096】(1) 各IPアドレス(IPサブネット含む)とポートの使用可否との管理テーブル(IPアドレス又はIPサブネットとアクセス許可/禁止情報とを対応させて登録したもの)104を内部に持っており、管理画面上からこの管理テーブルの設定ができる。ここで、IPサブネットは、IPアドレスと有効ビットマスク値とを組とするものであり、このIPサブネットを用いて複数のIPアドレスを指定することができる。

【0097】(2) ネットワーク中継機器からIPアドレスが送信された場合、管理テーブル104からIPアドレスを検索し、アクセス許可またはアクセス禁止を示す情報を前記ネットワーク中継機器に返信する。

【0098】(3) 受信したIPアドレスと一致するIPアドレスが管理テーブル104に登録されていない場合、管理テーブル104に登録されているIPサブネットの中で、適合する最もサブネットマスク長が長いIPサブネットを検索し、このIPサブネットに対応するア

クセス許可/禁止情報を前記ネットワーク中継機器に返信する。

【0099】(4) ネットワーク中継機器からの問い合わせ及びその問い合わせに対する返信の内容をログとして記録する。このログは、管理画面から参照できる。

【0100】図4を用いて、より具体的な流れを説明する。

【0101】ネットワーク中継機器101の1番ポート～4番ポート及びネットワーク中継機器102の1番ポート、3番ポート～5番ポートは、自動使用可否設定ポートに設定されているものとする。ネットワーク中継機器101の5番ポート及びネットワーク中継機器102の2番ポートは、自機及び接続される端末が上位ネットワークと通信できるように使用可能に設定されているものとする。

【0102】また、ネットワーク中継機器101、102には、IPアドレスの送信先となるネットワーク管理装置のアドレスとしてネットワーク管理装置103のアドレスが設定されているものとする。

【0103】ネットワーク管理装置103には、図示のように、予め内部の管理テーブル104に設定がなされているものとする。

【0104】いま、IPアドレスが172.17.33.1の端末105がネットワーク中継機器101の1番ポートに接続されたとする。端末105からフレームが送信されると、ネットワーク中継機器101のフィルタリングテーブルにフレームから抽出した端末105のMACアドレスが登録される。そのタイミングでネットワーク中継機器101は、IPアドレスを検出し、そのIPアドレスをネットワーク管理装置103に送信する。

【0105】ネットワーク管理装置103は、受信したIPアドレスに対応したデータを管理テーブル104から検索する。IPアドレス172.17.33.1は、アクセスが許可と設定されているので、ネットワーク管理装置103は、アクセス許可を示す情報をネットワーク中継機器101に返信する。

【0106】アクセス許可を示す情報を受信したネットワーク中継機器101は、端末105が接続されている1番ポートを使用可能にする。これにより、端末105は、ネットワーク中継機器101を介してネットワークにアクセスすることができるようになる。

【0107】同様に、この端末105がネットワーク中継機器102の3番ポートに接続された場合も、ネットワーク中継機器102の3番ポートは利用可能に設定される。つまり、この端末105は、どのネットワーク中継機器のどのポートに接続しても、ネットワークにアクセスすることができることになる。

【0108】端末105のIPアドレスが172.17.33.2の場合、管理テーブル104にアクセスが



禁止と設定されているので、ネットワーク中継機器 101, 102 からの問い合わせに対してネットワーク管理装置 103 からアクセス禁止を示す情報が返信される。アクセス禁止を示す情報を受信したネットワーク中継機器 101, 102 は、端末 105 が接続されているポートを使用不可にする。これにより、端末 105 は、ネットワーク中継機器 101, 102 を介してネットワークにアクセスすることができない。

【0109】端末 105 の IP アドレスが 172. 17. 33. 3 の場合、管理テーブル 104 に一致する IP が登録されていない。この場合、適合する IP サブネットであって最もサブネットマスク長が長い IP サブネットのデータが使用される。従って、172. 17. 33. 3 については、172. 17. 33. \* / 24 の IP サブネットがこの条件に適合するので、対応するアクセス許可を示す情報が返信される。

【0110】同様に、端末 105 の IP アドレスが 171. 1. 1. 1. の場合は、IP サブネット 171. \*. \*. \* / 8 が適合し、アクセス許可を示す情報が返信される。端末 105 の IP アドレスが 170. 1. 1. 1. の場合は、IP サブネット \*. \*. \*. \* / 0 が適合し、アクセス禁止を示す情報が返信される。

【0111】以上のネットワーク中継機器からの問い合わせ及び返信の内容はネットワーク管理装置 103 に記録され、後に管理者がそのログを管理画面から参照することができる。

【0112】ネットワーク中継機器 101, 102 とネットワーク管理装置 103 との通信ができなかった場合など、IP アドレスの送信に対する返信がなかった場合、ネットワーク中継機器 101, 102 は、このような場合のために予め指定してあった通りにポートの使用可否を設定する。

【0113】このようにして設定されたネットワーク中継機器の構成情報は、メモリ 209 に格納され、中継回路 207 によって通信処理に使用される。

#### 【0114】4) 第四の実施形態

図 5 に示されるように、本発明に係るネットワーク管理システムは、本発明に係る 2 台のネットワーク中継機器 101, 102 と、本発明に係るネットワーク管理装置 103 とを有する。ネットワーク中継機器は、例えば、スイッチングハブであり、図 2 に示した内部構成を有する。

【0115】以下に、スイッチングハブ 201 等のネットワーク中継機器が行う処理及びネットワーク中継機器に対して管理者が行う処理を示す。

【0116】(1) 管理者は、予めポート毎に、端末が接続された場合に、その端末の MAC アドレスを端末情報としてネットワーク管理装置に送信するかどうかを設定しておく。端末情報を送信するポートを以下、自動使用可否設定ポートと呼ぶ。

【0117】(2) 管理者は、自動使用可否設定ポートでないポートについて、その使用可否を予め設定しておく。

【0118】(3) 管理者は、MAC アドレスの送信先となるネットワーク管理装置のアドレスを予め設定しておく。

【0119】(4) ネットワーク中継機器は、フィルタリングテーブル (図示せず) に新たに MAC アドレスが登録される場合など、端末の MAC アドレスを送信するべき際、自動使用可否設定ポートが受信したフレームから端末の MAC アドレスを検出し、その MAC アドレスをネットワーク管理装置に送信する。

【0120】(5) ネットワーク中継機器は、MAC アドレスの送信に対する返信としてネットワーク管理装置からアクセス許可を示す情報を受信した場合、端末が接続されているポートを使用可能に設定する。

【0121】(6) ネットワーク中継機器は、MAC アドレスの送信に対する返信としてネットワーク管理装置からアクセス禁止を示す情報を受信した場合、端末が接続されているポートを使用不可に設定する。

【0122】(7) ネットワーク中継機器は、ネットワーク管理装置に MAC アドレスを送信した後、ネットワーク管理装置から返信がなかった場合、この場合のために予め指定してあったとおりに使用可否の設定を行う。

【0123】(8) 以上によって設定されたネットワーク中継機器の構成情報はメモリ 209 に格納される。爾後、中継回路 207 は、ネットワーク中継機器 201 の構成情報を通信処理に使用する。

【0124】以下に、ネットワーク管理装置 103 が行う処理を示す。

【0125】(1) 各 MAC アドレスとポートの使用可否との管理テーブル (MAC アドレスとアクセス許可 / 禁止情報とを対応させて登録したもの) 104 を内部に持っており、管理画面上からこの管理テーブルの設定ができる。

【0126】(2) ネットワーク中継機器から MAC アドレスが送信された場合、管理テーブル 104 から MAC アドレスを検索し、アクセス許可またはアクセス禁止を示す情報を前記ネットワーク中継機器に返信する。

【0127】(3) ネットワーク中継機器からの問い合わせ及びその問い合わせに対する返信の内容をログとして記録する。このログは、管理画面から参照できる。

【0128】図 5 を用いて、より具体的な流れを説明する。

【0129】ネットワーク中継機器 101 の 1 番ポート ~ 4 番ポート及びネットワーク中継機器 102 の 1 番ポート、3 番ポート ~ 5 番ポートは、自動使用可否設定ポートに設定されているものとする。ネットワーク中継機器 101 の 5 番ポート及びネットワーク中継機器 102 の 2 番ポートは、自機及び接続される端末が上位ネット

ワークと通信できるように使用可能に設定されているものとする。

【0130】また、ネットワーク中継機器 101, 102 には、MAC アドレスの送信先となるネットワーク管理装置のアドレスとしてネットワーク管理装置 103 のアドレスが設定されているものとする。

【0131】ネットワーク管理装置 103 には、図示のように、予め内部の管理テーブル 104 に設定がなされているものとする。

【0132】いま、MAC アドレスが 11:11:11:11:11:11 の端末 105 がネットワーク中継機器 101 の 1 番ポートに接続されたとする。端末 105 からフレームが送信されると、ネットワーク中継機器 101 のフィルタリングテーブルにフレームから抽出した端末 105 の MAC アドレスが登録される。そのタイミングでネットワーク中継機器 101 は、その MAC アドレスをネットワーク管理装置 103 に送信する。

【0133】ネットワーク管理装置 103 は、受信した MAC アドレスに対応したデータを管理テーブル 104 から検索する。MAC アドレス 11:11:11:11:11:11 は、アクセスが許可と設定されているので、ネットワーク管理装置 103 は、アクセス許可を示す情報をネットワーク中継機器 101 に返信する。

【0134】アクセス許可を示す情報を受信したネットワーク中継機器 101 は、端末 105 が接続されている 1 番ポートを使用可能にする。これにより、端末 105 は、ネットワーク中継機器 101 を介してネットワークにアクセスすることができるようになる。

【0135】同様に、この端末 105 がネットワーク中継機器 102 の 3 番ポートに接続された場合も、ネットワーク中継機器 102 の 3 番ポートは利用可能に設定される。つまり、この端末 105 は、どのネットワーク中継機器のどのポートに接続しても、ネットワークにアクセスすることができることになる。

【0136】端末 105 の MAC アドレスが 22:22:22:22:22:22 の場合、管理テーブル 104 にアクセスが禁止と設定されているので、ネットワーク中継機器 101, 102 からの問い合わせに対してネットワーク管理装置 103 からアクセス禁止を示す情報が返信される。アクセス禁止を示す情報を受信したネットワーク中継機器 101, 102 は、端末 105 が接続されているポートを使用不可にする。これにより、端末 105 は、ネットワーク中継機器 101, 102 を介してネットワークにアクセスすることができない。

【0137】端末 105 の MAC アドレスが 44:44:44:44:44:44 の場合、管理テーブル 104 に該当する MAC アドレスが登録されていないため、管理テーブル 104 の“その他”のデータが参照され、そのデータにはアクセスが禁止と設定されているので、ネットワーク中継機器 101, 102 からの問い合わせ

に対してネットワーク管理装置 103 からアクセス禁止を示す情報が返信される。ネットワーク中継機器 101, 102 は、端末 105 が接続されているポートを使用不可にするので、端末 105 は、ネットワーク中継機器 101, 102 を介してネットワークにアクセスすることができない。これにより、不明な MAC アドレスの端末をネットワークにアクセスさせることを防ぐことができる。

【0138】以上のネットワーク中継機器からの問い合わせ及び返信の内容はネットワーク管理装置 103 に記録され、後に管理者がそのログを管理画面から参照することができる。

【0139】ネットワーク中継機器 101, 102 とネットワーク管理装置 103 との通信ができなかった場合など、MAC アドレスの送信に対する返信がなかった場合、ネットワーク中継機器 101, 102 は、このような場合のために予め指定してあった通りにポートの使用可否を設定する。

【0140】このようにして設定されたネットワーク中継機器の構成情報は、メモリ 209 に格納され、中継回路 207 によって通信処理に使用される。

【0141】

【発明の効果】本発明は次の如き優れた効果を発揮する。

【0142】(1) ホスト名(識別キー)、ユーザ ID、IP アドレス、MAC アドレス等の端末情報によって認証されている端末のみがネットワークにアクセスできるようになり、ネットワークのセキュリティを確保することができる。

【0143】(2) 各端末毎或いは端末を利用するユーザ毎にポートの利用可否を統合管理することができる。

【0144】(3) ポート毎の接続端末の情報や利用可否設定のログを参照することができる。

【0145】(4) 利用可否を管理するネットワーク管理装置のアドレスを自由に設定することができる。

【0146】(5) 本発明によるポートの利用可否の設定を全ポートで使用しないこともできる。

【0147】(6) 本発明によるポートの利用可否の設定をポート毎に使用するか否かを設定できる。

【0148】(7) 端末情報の送信に対するネットワーク管理装置からの返信がなかった場合に端末が接続されているポートの使用可否をどうするかを予め指定しておくことができる。

【図面の簡単な説明】

【図 1】本発明の第一の実施形態を示すネットワーク管理システムの構成図である。

【図 2】本発明のネットワーク中継機器の実施形態を示すスイッチングハブの内部構成図である。

【図 3】本発明の第二の実施形態を示すネットワーク管理システムの構成図である。

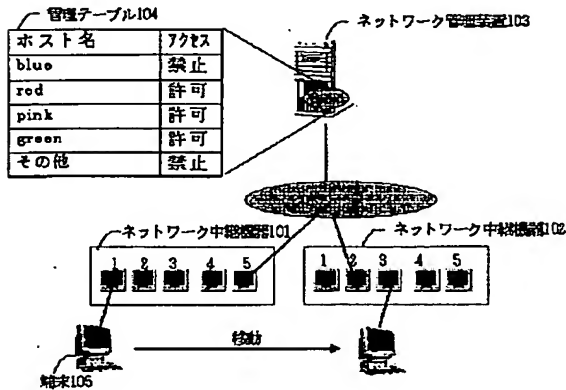
17

【図 4】本発明の第三の実施形態を示すネットワーク管理システムの構成図である。

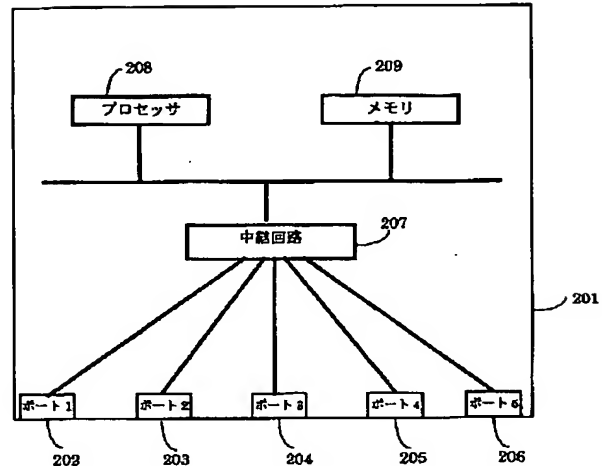
【図 5】本発明の第四の実施形態を示すネットワーク管理システムの構成図である。

【符号の説明】

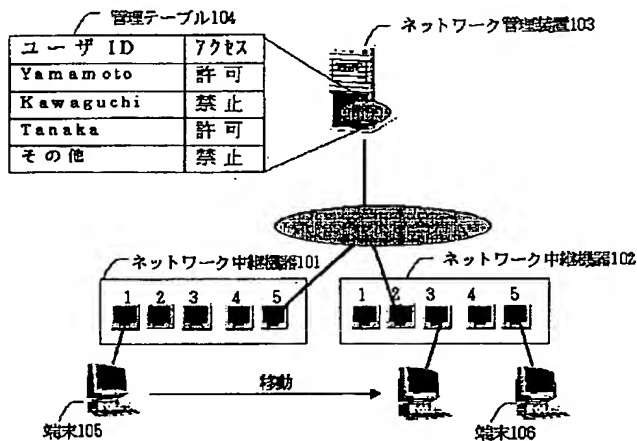
【図 1】



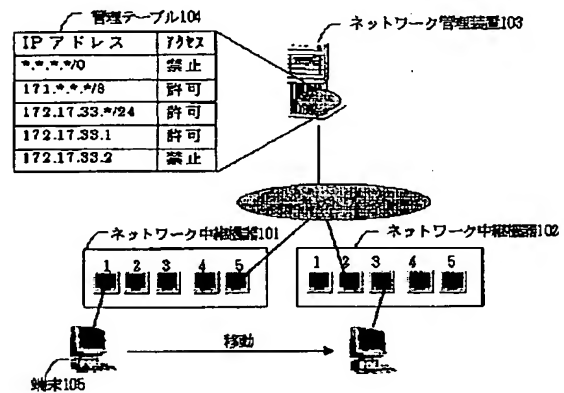
【図 2】



【図 3】



【図 4】



【図 5】

